Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

An OFAC Compliance Checklist For Ransomware Payments

By **John Reed Stark** (February 2, 2021, 5:43 PM EST)

John Reed Stark

Determining the bona fides of a ransomware attacker is like trying to confirm the height and weight of a poltergeist.

Yet that is precisely what the U.S. government expects ransomware victim companies to do before making a ransomware payment.

U.S. law generally prohibits facilitating, enabling, tendering, etc. payment to a suspected terrorist or someone located in, or affiliated with, a jurisdiction subject to comprehensive U.S. sanctions — such as Iran and North Korea.

Regrettably, a ransomware attacker could very well fall into any or all of those prohibited categories, so paying a ransomware attacker can expose the victim to violations of U.S. sanctions laws.

But proving the negative — i.e., that a ransomware attacker is not a terrorist or affiliated with a sanctioned country — is easier said than done.

First off, ransomware attackers are, by definition, liars, thieves, extortionists and members of a global criminal enterprise. Second, ransomware attackers have undertaken extreme technological measures to conceal any trace of their identity and location.

The options for ransomware victims are paralyzing. On the one hand, not paying the ransom — typically in bitcoin — to a ransomware attacker, who is holding the victim's data hostage and/or threatening to dump their data into social media, could mean financial ruin and even loss of life.

On the other hand, paying the ransom could result in costly government investigations, severe civil penalties and even prison for those involved with the payment.

The reality is that ransomware attacks can trigger a litany of anticipated and unanticipated consequences for victim companies — including millions of dollars in related costs and expenses, unquantifiable potential liabilities, overwhelming management drag, significant operational and reputational damage, and even death.

As a result, paying ransomware attackers, and rolling the dice about the legal consequences, has unfortunately become as routine a cost of business as paying the electric bill. It's become ransomware's dirty little secret: Most corporate victims pay the ransom.[1]

However, this current ransomware payment trend could shift in 2021.

A recent U.S. Department of the Treasury bulletin suggests heightened U.S. government scrutiny of ransomware payments in 2021, and ransomware victims should take substantial steps to steer clear of any U.S. government crackdown. But how?

This article suggests that by following the ransomware due diligence checklist set forth below, a ransomware victim who opts to pay the ransom can in the least mitigate the chances of a U.S. civil enforcement action or criminal prosecution, and perhaps even avoid U.S. government scrutiny altogether.

Some Background

Historically, ransomware attackers employed a type of malicious software designed to block access to a computer system or computer files until an extortion demand is paid.

Now, in addition, by licensing their criminal wares to franchisees who can then orchestrate ransomware-as-service attacks,[2] the threat is no longer merely the kidnapping of data but also the public release of that data via social media.

To further pressure the victim, a ransomware attacker might even flood a website or network with more requests than it can handle by executing a distributed denial of service, or DDoS, attack, rendering the company inaccessible.[3]

Indeed, the continuing success of ransomware attacks has spawned large, central, sophisticated cybercriminal organizations operating within a new and emerging criminal ecosystem consisting of an army of global threat actors using a dangerously evolving arsenal of high-tech intrusion appliances.

Extortion innovation is now an industry within itself as ransomware attackers have sharpened their business models, including guaranteeing turnaround times, providing real-time chat support for victims and offering payment demands customized to a victim's financial profile.

When it comes to ransomware attacks, there has perhaps never before in history been a crime that law enforcement seems so powerless to prevent, investigate, prosecute and bring to justice. Meanwhile, threat actors associated with rival nations such as Iran and North Korea have adopted ransomware attacks as a fast and easy means to bypass U.S. economic sanctions and funnel badly needed capital into their cash-starved economies.

OFAC Concerns

Given the anonymity of ransomware attackers and that most ransomware attackers demand their extortion payment in cryptocurrency, ransomware victims rarely learn the identity of ransomware attackers. This presents a problem because U.S. law generally prohibits making payments to those who are enemies of the U.S, such as terrorist organizations.

The U.S. Treasury's Office of Foreign Assets Control supervises the enforcement of these sanctions laws, such as the Trading with the Enemy Act[4] and the International Emergency Economic Powers Act, or IEEPA[5]

Under these acts, ransom payments — whether directly or indirectly through an intermediary — to foreign terrorist organizations[6] or specially designated global terrorists[7] identified by OFAC,

are illegal under U.S. law.

Monetary contributions to foreign terrorist organizations are considered material support under Title 18 of the U.S. Code, Section 2339B,[8] while transfers to specially designated global terrorists are violations of economic sanctions imposed pursuant to the IEEPA.

OFAC may impose steep civil penalties of up to $20 million for sanctions violations based on strict liability, meaning that, "a person subject to U.S. jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that was prohibited under sanctions laws and regulations administered by OFAC."[9]

The OFAC Advisory

Given the now common practice of making ransomware payments, on Oct. 1, 2020, OFAC issued a formal advisory about the sanctions risks of facilitating ransomware payments.[10]

The OFAC advisory, titled, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," focuses on potential sanctions risks for those involved in ransomware payments to bad actors, including ransomware victims and those acting on their behalf, such as "financial institutions, cyber-insurance firms, and companies involved in digital forensics and incident response."[11]

OFAC stresses that ransomware payments, including payments to digital currency wallets or addresses, can be a violation of economic sanctions laws and not only represent a threat to national security, but also create a moral hazard, encouraging future attacks.

Although the OFAC advisory does not mention potential liability of attorneys who help facilitate ransomware payments, Kaveh Miremadi, section chief in OFAC's enforcement division, said recently that in the context of a ransomware payment, lawyers could be culpable for OFAC violations, and may even be held to a higher standard.[12]

An OFAC Ransomware Due Diligence Checklist

The OFAC advisory and another from the U.S. Financial Crimes Enforcement Network that was issued the same day do not introduce any new rules or regulations, but both nonetheless serve as a stark reminder that ransomware payments have become of serious concern to the U.S. federal government and will likely experience heightened U.S. governmental scrutiny going forward.

Along these lines, set forth below is a ransomware due diligence checklist for ransomware victims who decide to pay the extortion demand. While not necessarily exhaustive, this checklist can provide a helpful road map for establishing the requisite mitigation and due diligence to avoid OFAC-related violations.

1. Build a ransomware response team.

After being hit by a ransomware attack, begin by engaging a legal team to quarterback the response, which can ensure communication lines are properly organized, thoughtfully orchestrated and, when appropriate, protected by the attorney-client and work product privileges.

The legal team can then, in turn, engage:

- A digital forensics firm to assist with investigation of the attack, restoration of backup files

and remediation. To investigate the ransomware attacker, the digital forensics team should have at their disposal a library of code similarities, shared tools, and shared infrastructure and targets of known ransomware attackers. To interface with law enforcement, regulators, vendors and other interested constituencies, it can help if the firm has on hand former federal law enforcement officials;

- An OFAC lawyer, who has either previously worked for OFAC or has been engaged in OFAC-related representations for many years;

- An experienced ransomware payment facilitator who has negotiated with ransomware attackers before and who can also expedite the bitcoin payment, including acquiring the demanded amount of bitcoin and confirming the bona fides of decryption keys, typically with a test key — i.e., proof of life — to kick off negotiations; and

- An experienced insurance lawyer who can manage and document all related insurance claims, who is familiar with the perils of so-called silent cyber,[13] and who can advocate for payment under cyber, property, general liability and/or any other relevant insurance policies.

2. Review the OFAC list.

The OFAC advisory warns against payments from U.S. persons to individuals or entities on its Specially Designated Nationals and Blocked Persons List, other blocked persons and those covered by comprehensive country or region embargoes.

Since 2016, OFAC has added high-profile entities, individuals and cryptocurrency wallet addresses associated with ransomware variants, including those associated with Cryptolocker, SamSam, WannaCry and Dridex malware, to the specially designated nationals list and continues adding entities to its list almost daily.

To assist companies conducting OFAC-related due diligence, OFAC maintains online the Consolidated Sanctions List and allows for email notifications of any updates.[14]

Companies should engage an expert who subscribes to the OFAC alerts, who is familiar with how to search and decipher the specially designated nationals list and who knows how to take advantage of the specially designated nationals list's dynamic search capabilities.[15]

3. Don't rely on an OFAC license application.

In situations in which a company wishes to engage in a financial transaction with a prohibited party, such as a terrorist nation, it is possible to request what is known as a license from OFAC authorizing such conduct.[16]

However, the OFAC advisory states that "license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial."

According to Miremadi, OFAC has not yet issued a license to a ransomware attack victim. This is not to say that issuing a license is not possible in an emergency situation, but it appears unlikely for now.

First off, the license application process would take too long, and OFAC would have to create a streamlined licensing process for ransomware situations. Moreover, OFAC generally refuses to issue licenses for theoretical or potential scenarios, or where U.S. jurisdiction is uncertain.

As an aside, self-reporting, and not a license application after-the-fact, remains the proper means of mitigating any payment that turns out to have been made to a terrorist organization or other prohibited recipient.

4. Notify and cooperate with law enforcement.

The OFAC advisory encourages victims of ransomware attacks to contact law enforcement immediately, noting that "self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus."

OFAC clearly acknowledges that such notification and cooperation while not necessarily an automatic safe harbor, certainly garners substantial mitigating credit.

One way to work with law enforcement, especially when it comes to ransomware, is to engage former federal criminal law enforcement agents, such as former FBI or U.S. Secret Service agents, who are familiar not just with the playing field but with the players as well.

5. Research the modus operandi.

In a targeted ransomware attack, an experienced threat hunter can glean sufficient threat intelligence from the tactics, techniques and protocols — e.g., the infrastructure typically targeted such as servers, virtual machines, cloud environments, databases, etc. — to make an educated guess on the geographical location or likely identity of the ransomware attackers.

Knowing the region can help with OFAC list analysis, because the sanctions lists are in some cases categorized by country.[17]

But while matching cyber modus operandi can certainly provide worthwhile intelligence fodder for U.S. government investigative teams and policymakers, pinpointing attribution to, and ascertaining the motives of, cyberattackers is far more art than science.

Too often it is a patchwork of hypothesizing, speculation, supposition and simple old-fashioned guesswork, rendering attribution conclusions overly subjective, skewed or even mistaken.

Thus, make sure to engage an experienced threat hunting team who will not only carefully document their procedures but will also stand strong behind their conclusions.

6. Beware of false flags.

Even if digital forensic investigators can triangulate a common modus operandi among attackers, the entire criminal design could all be a false flag subterfuge, where one country's cyber gang coopts the practices of another country's cyber gang, to confuse, misdirect and lead astray.

From simply issuing false claims of responsibility to emulating the tools, techniques and even

languages typically used by the group or country, false flag cyberattackers can deceive, interfere and trick even the most seasoned cyber experts.

By interjecting chaos and confusion during a digital forensic investigation of a ransomware attack, false flags make an already problematic undertaking even more byzantine.

False flags can also obfuscate motive. Collecting a ransom may not be the only possible motive behind a cyberattack. Governmental destruction, espionage, terrorism, financial crime, insider trading, intellectual property thievery, trade secret pilfering, extortion and market manipulation — just to name a few — are all potential ransomware attack objectives.

Consider adding specific documentation which addresses the issue of a possible false flag, and confirm that the digital forensics team has expertise along those lines.

7. Consult with OFAC if possible.

OFAC encourages ransomware victims and companies involved in helping victims to "contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus."

OFAC also urges victims to contact the U.S. Treasury's Office of Cybersecurity and Critical Infrastructure Protection if the incident involves a U.S. financial institution or could cause a significant disruption involving a critical financial service.

By engaging with OFAC, a ransomware victim can further mitigate any potential future OFAC enforcement action.

8. Create and update OFAC risk-based compliance programs.

The OFAC advisory notes that companies that engage with victims of ransomware attacks should implement a risk-based compliance program to mitigate exposure to sanctions-related violations, to "account for the risk that a ransomware payment may involve a specially designated national or blocked person, or a comprehensively embargoed jurisdiction."

This can become a challenging endeavor. First off, attackers can hijack internet protocol addresses to obfuscate their true location.

Second, unlike more traditional transactions where all parties to a transaction are known to each other, one party to a ransomware payment transaction is making every effort to conceal their identity.

Finally, there is not much time to facilitate a ransomware payment, and victims are reluctant to ask for extensions. Nonetheless, a seasoned OFAC attorney can provide some risk-compliance guidance, in writing, which could serve as a mitigating factor should OFAC consider an enforcement action.

9. Tap into an insurance company's expertise.

Many companies who experience ransomware attacks have little experience with OFAC and the complex compliance procedures required for a successful sanctions program. But insurance companies, which are already heavily regulated — akin to financial institutions — often have seasoned OFAC-related experience as well as veteran anti-money laundering expertise.

More and more insurance companies maintain built-in ransomware negotiation teams and OFAC

specialists that can add substantial value to understanding, and meeting, OFAC-related compliance responsibilities.

10. Engage the board of directors.

Once a ransomware attack hits, the C-suite should immediately engage its board of directors, and draw upon the board's wisdom and proficiency to manage the situation. Every ransomware attack is a bet-the-company situation, which warrants board oversight, scrutiny and immersion.

11. File a suspicious activity report if appropriate.

On the same date as the OFAC advisory, FinCEN issued its own ransomware-related advisory, titled, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," highlighting the role of financial intermediaries in payments, ransomware trends and typologies, related financial red flags, and effective reporting and information sharing related to ransomware attacks.[18]

The FinCEN advisory reminds financial institutions about their obligations under the Bank Secrecy Act to report suspicious activity,[19] including ransomware payments in so-called suspicious activity reports — a form that financial institutions, and those associated with their business, must file with FinCEN whenever there is a suspected case of money laundering or fraud.[20]

Along these lines, FinCEN's advisory contains a list of 10 "red flag indicators of ransomware related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks."

12. Maintain a paper trail.

Be ready to be accountable, which entails creating a carefully managed paper trail of deliberations, consultations, activities, etc. Document not just the due diligence and other legalities triggered by a ransomware response but also the extraordinary duress, including the rationale for making the payment.

It is not lost on OFAC officials that companies who refuse to pay ransomware attackers can face severe economic and even existential consequences, and, in the case of health care companies such as hospitals, can potentially lead to loss of life, as reportedly occurred recently with a ransomware attack on a hospital in Germany.[21]

Looking Ahead

No matter how sophisticated and vigilant, no company can ever enjoy immunity from a cyberattack.

Of course, there are technologies and processes to help prevent and detect ransomware attacks, including:

- Establishing better training, especially relating to phishing schemes;

- Installing sturdier remote desktop and email controls;

- Limiting administrative accounts;

- Initiating frequent software patching;

- Employing the latest endpoint response, malware and lateral detection tools;

- Requiring stronger passwords and two factor authentication; and

- Utilizing a well-governed and properly configured security information and event management system.[22]

The list could go on.

But too many companies cannot afford robust cybersecurity systems, cannot compete for the limited talent pool of cyber professionals — e.g. hospitals, schools and municipalities — or, for whatever reason, simply remain less inclined to step up their online infrastructure and virtual governance.

Sadly, unless the U.S. government takes dramatic action — such as curtailing the flow of bitcoin, which serves as the lifeblood of ransomware attackers[23] — ransomware attacks will become even more numerous, sophisticated and costly.

To make matters worse, the COVID-19 pandemic has resulted in more employees working from home, thereby creating even more opportunities for online threat actors.[24] Hence, the disturbing trend of paying off ransomware attackers will likely continue into 2021 and perhaps even beyond.

Meanwhile, given the OFAC and FinCEN advisories, the U.S. government has signaled heightened scrutiny of not just the companies making ransomware payments but also the various persons and consultants facilitating the bitcoin transfer — including digital forensic firms, ransomware remediation firms, cyberinsurers — even the cyber-lawyers providing advice throughout the process.

But the news is not all bad. Although ransomware victims can find themselves victimized twice — first by the ransomware attacker and second by the U.S. government in the form of an OFAC enforcement action — my take is that if ransomware victims follow the ransomware due diligence checklist presented herein, they might just avoid such an unfair and devastating double whammy.

John Reed Stark is president at John Reed Stark Consulting LLC and senior lecturing fellow at Duke University Law School. He previously served for almost 20 years in the U.S. Securities and Exchange Commission's Division of Enforcement, the last 11 of which as chief of its Office of Internet Enforcement.

firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.linkedin.com/pulse/ransomwares-dirty-little-secret-most-victims-pay-john-reed-stark/.

[2] https://www.natlawreview.com/article/regulatory-crackdown-ransomware.

[3] https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/amp/.

[4] https://www.law.cornell.edu/uscode/text/50/chapter-53.

[5] https://www.law.cornell.edu/uscode/text/50/chapter-35.

[6] https://www.state.gov/foreign-terrorist-organizations/.

[7] https://www.state.gov/executive-order-13224/.

[8] https://www.law.cornell.edu/uscode/text/18/2339B.

[9] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[10] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[11] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

[12] https://docketevents.com/de/live/29/page/259.

[13] https://btlaw.com/insights/events/silent-cyber-viewing-cyber-as-a-peril.

[14] https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list-data-files.

[15] https://sanctionssearch.ofac.treas.gov.
[16] https://home.treasury.gov/policy-issues/financial-sanctions/ofac-license-application-page.

[17] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information.

[18] https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

[19] https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html.

[20] https://www.fincen.gov/suspicious-activity-reports-sars.

[21] https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/.

[22] https://www.aon.com/cyber-solutions/thinking/consider-these-10-critical-steps-to-prevent-and-detect-ransomware-threats/?utm_source=elevate&utm_medium=social&utm_campaign=ca-2021-crs-cyber-social&utm_content=english&_lrsc=56422fee-a6e7-461e-b578-

7e011ba3fa0d&utm_source=Linkedin_Elevate.

[23] https://www.linkedin.com/pulse/proposed-2021-biden-ransomware-crackdown-john-reed-stark/.

[24] https://www.cisa.gov/telework.
